# CLAIMS

1. A method for providing secure authentication of a user to a system and secure operation of the system thereafter, the method comprising:

authenticating a user to the system directly or via a proximity device;

authenticating the proximity device to a receiver in the system;

upon successful authentication, initiating operation of the system; and

intermittently communicating between the proximity device and the receiver to verify whether the proximity device is within continued proximity of the system.

2. The method of claim 1, further comprising:

if the user is not authenticated to the proximity device after a predetermined number of attempts, garbling sensitive information stored in the proximity device.

3. The method of claim 1, further comprising:

communicating a distress signal, if it is determined that the proximity device is not operating in proximity of the system.

4. The method of claim 1, further comprising:

beginning operation of the system in a fail-safe mode if it is determined that the proximity device is not operating in proximity of the system.

5. The method of claim 1, wherein the proximity device is one of the following: a personal digital assistant (PDA), a cellular phone, a pager, a smart card, a pocket PC, an audio-video device, a laptop, a tablet PC, a camera, or a portable device carried by a courier.

6. The method of claim 1, wherein authenticating the user to the system or to the proximity device comprises at least one or a combination of the following: receiving user identification (ID) information, scanning the user's finger print, recognizing the user's facial characteristics, recognizing the user's voice, verifying a user's DNA, and verifying biometrics of the user.

7. The method of claim 1, wherein authenticating the proximity device to the receiver comprises at least one or a combination of the following: a challenge-response algorithm, a digital signature algorithm, a public-private key algorithm, a one-time password algorithm, and a symmetric key algorithm.

8. The method of claim 1, wherein authenticating the proximity device to the receiver comprises one of: communicating via a wireless interface or via a wired interface.

9. A system for user authentication to a machine and secure operation of the machine thereafter, the system comprising:

a receiver coupled to, or integrated with, the machine; and

a proximity device, comprising;

means for authenticating a user to the proximity device;

means for authenticating the proximity device to the receiver; and

means for, upon successful authentication, intermittently communicating between the proximity device and the receiver to verify whether the proximity device is within proximity of the machine.

10. The system of claim 9, wherein the receiver comprises:

means for determining whether the proximity device is in proximity of the machine; and

means for beginning operation of the machine in a fail-safe mode if it is determined the proximity device is no longer operating within proximity.

11. The system of claim 10, wherein the receiver further comprises:

means for initiating communication of a distress signal to a receiving station upon beginning operation in a fail-safe mode.

12. The system of claim 9, wherein the proximity device is one of the following: a personal digital assistant (PDA), a cellular phone, a pager, a smart card, a pocket PC, an audio-video device, a laptop, a tablet PC, a camera, or a portable device carried by a courier.

13. The system of claim 9, wherein the means for authenticating a user to the proximity device comprises at least one of the following: means for receiving user identification (ID) information, means for scanning the user's finger print, means for recognizing the user's facial characteristics, means for recognizing the user's voice, means for verifying a user's DNA, means for recognizing body temperature, means for recognizing blood pressure, and means for verifying biometrics of the user.

14. The system of claim 9, wherein the means for authenticating the proximity device to the receiver comprises at least one of the following: means for processing a challenge-response algorithm, means for processing a digital signature algorithm, means for processing a public-private key algorithm, means for processing a one-time password algorithm, means for processing the identity of the user, and means for processing a symmetric key algorithm.

15. The system of claim 9, wherein the proximity device further comprises:

means for storing identification information about at least a first user.

16. A device for providing authentication of a user to a system and for providing secure operation of the system thereafter, the device comprising:

memory for storing identification information of at least a first user;

an interface for authenticating a user;

an interface for authenticating the device to a receiver integrated with the system; and

logic configured to intermittently communicate with the receiver upon successful authentication.

17. The device of claim 16, wherein the interface for authenticating the device to the receiver is a wireless interface.

18. The device of claim 16, wherein the interface for authenticating the device to the receiver is a wired interface.

19. The device of claim 16, further comprising:

logic configured to garble secure information upon a predetermined number of failed attempts at authenticating the user.

20. The device of claim 16, further comprising:

logic configured to operate the device in a sleep mode, such that minimal power needed to maintain intermittent communications with the receiver is utilized.